Informe de Auditoría Técnica de Seguridad - Aplicación Web de Entidad Pública

1 introducción

Este documento presenta los resultados de una auditoría técnica de seguridad realizada a la aplicación web de la entidad. El objetivo principal fue identificar y evaluar vulnerabilidades que pudieran comprometer la integridad, confidencialidad y disponibilidad del sistema. Los hallazgos se clasifican por su nivel de criticidad y se acompañan de recomendaciones prácticas para su mitigación.

2 tabla de Hallazgos

Hallazgo	Impacto	Criticidad	Recomendación
Uso de credenciales por defecto	Acceso administrativo no autorizado	Alta	Cambiar credenciales y reforzar políticas de autenticación
Exposición de trazas internas	Revelación de rutas, clases y lógica interna del sistema	Media	Configurar manejo de errores personalizado
API sin autenticación	Acceso libre a datos sensibles	Alta	Implementar autenticación y control de acceso

Exportar a Hojas de cálculo

Redacción técnica detallada del hallazgo: API sin autenticación

3.1. Descripción del Hallazgo

La API pública de la aplicación no implementa mecanismos de autenticación ni control de acceso para las solicitudes de tipo

GET. Esto permite que cualquier usuario o atacante acceda a datos sensibles de manera no autorizada, sin necesidad de credenciales.

2.2. Método de Prueba y Evidencia

- **Herramienta utilizada:** Burp Suite Professional.
- **Método de prueba:** Se interceptó una solicitud GET a la API (/api/v1/datos_sensibles) y se reenvío al módulo Repeater de Burp Suite para su

manipulación. Se modificaron los parámetros y se observó que el servidor respondía con información sensible sin validar ningún token de sesión o credenciales de usuario.

- **Evidencia resumida:** La solicitud curl a continuación muestra la vulnerabilidad. La respuesta del servidor (HTTP/1.1 200 OK) contiene datos sensibles sin requerir autenticación.

```
curl -X GET "https://ejemplo.com/api/v1/datos_sensibles"

// Respuesta
{
"id": 12345,
"nombre_cliente": "Juan Pérez",
"saldo_cuenta": 1500000,
"info_confidencial": "..."
}
```

3.3. Recomendación Técnica Detallada

Se recomienda implementar un robusto sistema de autenticación y control de acceso en la API. Esto incluye:

1. **Autenticación:** Implementar un esquema de autenticación como tokens JWT (JSON Web Tokens) o claves API para validar la identidad de cada solicitud.
2. **Autorización:** Tras la autenticación, aplicar un control de acceso estricto que valide si el usuario autenticado tiene los permisos necesarios para acceder a los datos o recursos solicitados.
3. **Principio del Mínimo Privilegio:** Asegurar que los endpoints solo devuelvan los datos estrictamente necesarios para la función requerida, limitando la exposición de información sensible.
4. **Validación de entrada:** A pesar de la autenticación, continuar validando y saneando todos los parámetros de entrada para prevenir otros ataques como la inyección de código SQL o la inyección de comandos.